U.S. Department of State
Privacy Impact Assessment Summary

TITLE: Waiver Review System (WRS) (subsystems: JWOL, ISCS)
May 2, 2007

I. Describe the information to be collected (e.g., nature and source). Be sure to include any information in an identifiable form, e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc).

Foreign National J Visa Waiver applicants provide the primary source of information for their J Visa waiver. J Visa waiver processing personnel may collect additional information from the applicant.

Data collected includes the applicant's title, surname; given name (first and middle name); maiden name; gender; date of birth; city of birth; country of birth; citizenship, country; and country of legal permanent residence.

II. Why is the information being collected (e.g., to determine eligibility)?

The information is collected for the initiation, handling, and tracking of J Visas waiver requests.

III. How will the information be used (e.g., to verify existing data)?

The information will be used to make decisions on whether or not to grant the waiver.

IV. Will you share the information with others (e.g., another agency for a programmatic purpose)? If yes, list the entities.

Yes, the Department of Homeland Security (DHS) will be able to access this data.

V. Describe what opportunities individuals have been given to decline to provide information or to consent to particular use of the information (e.g., whether individual may withhold permission for a particular use).

Official forms used to collect applicant data that is entered into the systems under this program are OMB approved and contain a Privacy Act statement. Specific information regarding how the data is used is contained in the Federal Register.

VI. How will the information be secured (e.g., administrative and technological controls)?

At a high-level, the following controls are in place to secure information processed by WRS:

- Windows and application level identification and authentication mechanisms
- Windows and application level access control lists
- Application level authentication and levels of privilege.
- End-user training
- Security training, including annual refresher courses
- Operating system, database, and application level security scanning
- Audit trails track the last changes made by the last user to access the system

For a detailed description of the management, operational, and technical controls in place to protect data processed by WRS, refer to the WRS System Security Plan.

VII. How will the data be retrieved (e.g., will it be retrieved by a personal identifier such as name, social security number, address, telephone number or some other identifier that is unique to an individual)?

A case number will be assigned to each application that is paid for and presented to the J-Visa waiver office. This case number can be used for retrieving case status on the ISCS subsystem website (which does not include personally identifiable information) and the WRS subsystem.